Statement of Leslie Harris
President/CEO, Center for Democracy & Technology
Before the Senate Commerce, Science & Transportation Committee

"Privacy Implications of Online Advertising"
July 9, 2008

Chairman Inouye and Members of the Committee:

On behalf of the Center for Democracy & Technology ("CDT"), I thank you for the opportunity to testify today. We applaud the Committee's leadership in examining the privacy impact of new online advertising models.

I. Summary

CDT recognizes that advertising is an important engine of Internet growth. Consumers benefit from a rich diversity of content, services and applications that are provided without charge and supported by advertising revenue. However, as sophisticated new behavioral advertising models are deployed, it is vital that consumer privacy be protected. Massive increases in data processing and storage capabilities have allowed advertisers to track, collect and aggregate information about consumers' Web browsing activities, compiling individual profiles used to match advertisements to consumers' interests. All of this is happening in the context of an online environment where more data is collected – and retained for longer periods – than ever before and existing privacy protections have been far outpaced by technological innovation.

Behavioral advertising represents a small but rapidly growing part of the online advertising market. Market research firm eMarketer reported last year that spending on behaviorally targeted online advertising is expected to reach $1 billion this year and to quadruple by 2011.[1] The recent spate of acquisitions of the online advertising industry's largest players by major Internet companies is powerful evidence that the online advertising marketplace is headed toward more data aggregation tied to a single profile – and one that may be more readily tied to a person's identity.[2] And while we have yet to see evidence that this new

[1] "Behavioral Advertising on Target … to Explode Online," *eMarketer* (Jun. 2007), http://www.emarketer.com/Article.aspx?id=1004989.

[2] No fewer than five major mergers and acquisitions have been completed in the last 18 months: Google purchased online advertising company DoubleClick, Inc.; WPP Group, a large ad agency, acquired the online ad company 24/7 Real Media; Yahoo! acquired ad firm RightMedia; Microsoft acquired online ad

advertising model will reap the promised rewards, it is already migrating from individual Web sites to the infrastructure of the Internet itself: In the last year, Internet Service Providers ("ISPs") have begun to form partnerships with ad networks to mine information from individual Web data streams for behavioral advertising. Ad networks that partner with ISPs could potentially collect and record every aspect of a consumer's Web browsing, including every Web page visited, the content of those pages, how long each page is viewed, and what links are clicked. Emails, chats, file transfers and many other kinds of data could all be collected and recorded.

The ISP model raises particularly serious questions. Thus far, implementations appear to defy reasonable consumer expectations, could interfere with Internet functionality, and may violate communications privacy laws.

Notwithstanding the recent growth of behavioral advertising, most Internet users today do not know that their browsing information may be tracked, aggregated and sold. After almost a decade of self-regulation, there is still a profound lack of transparency associated with these practices and an absence of meaningful consumer controls.

There are several efforts underway to respond to the new online advertising environment. First, the Federal Trade Commission staff recently released a draft of proposed principles for self-regulation, which represent a solid step forward. However, it is not clear whether the FTC will formally adopt the principles or put its enforcement power behind them.

The Network Advertising Initiative ("NAI") is also in the process of revising its guidelines. This is a welcome but long-overdue development. Unfortunately, self-regulation has not worked to date and, even if strengthened, will never by itself fully protect consumers' privacy interests.

Congress needs to take a comprehensive look at the current and emerging practices associated with behavioral advertising and the risks those practices pose to consumer privacy and control. We recommend that Congress take the following steps to address the significant privacy concerns raised by behavioral advertising:

- The Committee should hold a series of hearings to examine specific aspects of behavioral advertising, in particular the growing involvement of ISPs, the use of sensitive information, and secondary uses of behavioral profiles.

---

service provider aQuantive; AOL purchased Tacoda, a pioneering firm in the area of behavioral advertising.

- The Committee should set a goal of enacting in the next year a simple, flexible baseline consumer privacy law that would protect consumers from inappropriate collection and misuse of their personal information, both online and offline.
- The Committee should strongly urge the Federal Trade Commission to exercise its full enforcement authority over online advertising practices.
- Congress should examine and strengthen existing communications privacy laws to cover new services, technologies and business models with consistent rules. The Electronic Communications Privacy Act ("ECPA") is decades old, and its application in today's online world is often unclear.
- Congress should encourage the FTC to investigate how technology can be harnessed to give consumers better control over their online information. Simple tools that put consumers in controls of their information, such as a "Do Not Track" list, deserve consideration.

II. Understanding Online Advertising Practices

Commercial Web sites that supply content to consumers free of charge are often supported by online advertising. These sites – known as "publishers" in the advertising world – make available certain portions of space on their pages to display ads. That space is sold to advertisers, ad agencies, or online ad intermediaries that find and place advertisements into the space. These intermediaries may also make arrangements to collect information about user visits to the publisher pages. Since very few publishers supply their own advertising, it is common that when a consumer visits a publisher site, the consumer's computer also connects to one or more advertisers, ad agencies, or ad intermediaries to send data about the consumer's visit to the site and receive the advertising on the site.

One type of ad intermediary is known as an "advertising network." At their most basic level, ad networks contract with many different publishers on one side and many different advertisers on the other. Armed with a pool of space in which to display ads on publisher sites, and a pool of ads to display, ad networks are in the business of matching up the two by using the data they collect about consumers' site visits.

A. Contextual Advertising

There are many different ways for an ad network to determine which advertisement should be placed in which space. The two most often discussed are "contextual" advertising and "behavioral" advertising. Contextual advertising, which is often used to generate ads alongside search results, matches advertisements to the content of the page that a consumer is currently viewing –

a consumer who visits a sports site may see advertisements for golf clubs or baseball tickets on that site.

The privacy risks associated with contextual advertising vary. If the practice is transparent to the user and data collection and retention is minimal, the practice poses little risk. By contrast, privacy concerns are heightened if the user data is retained in an identifiable or pseudonymous form (i.e., linked to a user identifier) for long periods of time even if it is not immediately used to create advertising profiles.

B. Behavioral Advertising

By contrast, behavioral advertising matches advertisements to the interests of the consumer as determined over time. If a consumer visits several different travel sites before viewing a news site, he or she might see a behaviorally targeted travel advertisement displayed on the news page, even if the news page contains no travel content. A traditional behavioral ad network builds up profiles of individual consumers by tracking their activities on publisher sites in the network (although this model is evolving, as we discuss below). When the consumer visits a site where the ad network has purchased ad space, the ad network collects data about that visit and serves an advertisement based on the consumer's profile. Diagrams illustrating this process are included in Appendix A.

Consumers' behavioral advertising profiles may incorporate many different kinds of data that are in and of themselves not personally identifiable. Many networks avoid linking profiles to what has traditionally been considered "personally identifiable information" ("PII"): names, addresses, telephone numbers, email addresses, and other identifiers. But as the comprehensiveness of consumer advertising profiles increases, the ability of marketers and others to link specific individuals to profiles is also growing. In 2006, for example, AOL released three months' worth of search queries generated by half a million users; in the interest of preserving users' anonymity, AOL replaced individuals' screen names with numbers. Based solely on search terms associated with one number, reporters at the New York Times were able to pinpoint the identity of the user who generated them.[3] The risk of supposedly non-personally identifying data

[3] Michael Barbaro and Tom Zeller, Jr., "A Face Is Exposed for AOL Searcher No. 4417749," *The New York Times* (Aug. 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&ex=1312776000&adxnnl=1&oref=slogin&adxnnlx=1215021816-j7kbrLxHU1hCdcMyNqHEbA.

being used to identify individuals has spurred several ad networks to take extra steps to de-identify or remove personal information from their data storage.[4]

Profiles may also be intentionally tied to PII. For example, data collected online by a merchant or by a service provider may permit an advertising profile to be tied to an individual's email account. Offline data may also be merged with online profiles. For years, data service companies have maintained profiles about consumers based on information gleaned from public sources such as property and motor vehicle records, as well as records from sources like catalog sales and magazine subscriptions. These data companies are now also entering the online advertising business, potentially allowing the linking of online and offline profiles.[5]

C. The Evolution of Behavioral Advertising – More Data, More Data Sources

As noted above, recent market consolidation facilitates more comprehensive data collection. Companies that run consumers' favorite Web-based services – Web search, Web mail, maps, calendars, office applications, and social networks – have all purchased behavioral advertising networks within the last year. In the past, major Internet companies could gather information about how an individual used its services and applications such as search, but did not have direct access to information about the user's other Web browsing habits. With the acquisition of behavioral advertising networks, these companies could potentially marry the rich data about an individual's use of one site with a broad view of his or her activities across the Web. The concerns about this aggregation of consumer data are heightened because many online companies retain data for months or years on end in identifiable or pseudonymous form, creating a host of privacy risks.

Finally, ad networks are now turning to the most comprehensive and concentrated source of information about Internet use: the individual Web data streams that flow through ISPs.[6] In this emerging model, the ISP intercepts or

---

[4] See, e.g., Microsoft, *Privacy Protections in Microsoft's Ad Serving System and the Process of "De-identification"* (Oct. 2007), http://download.microsoft.com/download/3/1/d/31df6942-ed99-4024-a0e0-594b9d27a31a/Privacy%20Protections%20in%20Microsoft%27s%20Ad%20Serving%20System%20and%20the%20Process%20of%20De-Identification.pdf.

[5] Acxiom runs Relevance-X, an online ad network. Last year Experian acquired the online data analysis company Hitwise. *See* Acxiom, *Acxiom: Relevance-X* (last visited Jul. 2008), http://www.acxiom.com/Relevance-X; Experian, "Acquisition of Hitwise" (Apr. 2007), http://www.experiangroup.com/corporate/news/releases/2007/2007-04-17b/.

[6] *See, e.g.,* Peter Whoriskey, "Every Click You Make," *The Washington Post* (Apr. 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule; Saul Hansell, "I.S.P. Tracking:

allows an ad network to intercept the content of each individual's Web data stream. The ad network then uses this traffic data for behavioral advertising, serving targeted ads to the ISP's customers on publisher sites as the customers surf the Web. We address the unique issues posed by this advertising model in detail below.

III. The Privacy Risks of Behavioral Advertising

Behavioral advertising poses a growing risk to consumer privacy; consumers are largely unaware of the practice and are thus ill equipped to take protective action. They have no expectation that their browsing information may be tracked and sold, and they are rarely provided sufficient information about the practices of advertisers or others in the advertising value chain to gauge the privacy risks and make meaningful decisions about whether and how their information may be used. In a recently released Harris Interactive/Alan F. Westin study, 59% of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services.[7] A recent TRUSTe survey produced similar results.[8] It is highly unlikely that these respondents understood that this type of ad targeting is already taking place online every day.

In most cases, data collection for behavioral advertising operates on an opt-out basis. Opt-out mechanisms for online advertising are often buried in fine print, difficult to understand, hard to execute and technically inadequate. Only the most sophisticated and technically savvy consumers are likely to be able to successfully negotiate such opt-out processes. Moreover, in most cases, opt-out mechanisms offered for behavioral advertising only opt the user out of receiving targeted ads, but do not opt the user out of data collection about his or her Internet usage.

The Mother of All Privacy Battles," *The New York Times: Bits Blog* (Mar. 2008) at http://bits.blogs.nytimes.com/2008/03/20/isp-tracking-the-mother-of-all-privacy-battles/?scp=1-b&sq=the+mother+of+all+privacy+battles&st=nyt.

[7] Alan F. Westin, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings* (Mar. 2008).

[8] TRUSTe, "TRUSTe Report Reveals Consumer Awareness and Attitudes About Behavioral Targeting" (Mar. 2008), http://www.marketwire.com/mw/release.do?id=837437&sourceType=1 ("71 percent of online consumers are aware that their browsing information may be collected by a third party for advertising purposes . . .. 57 percent of respondents say they are not comfortable with advertisers using that browsing history to serve relevant ads, even when that information cannot be tied to their names or any other personal information.").

For behavioral advertising to operate in a truly privacy-protective way, data collection needs to be limited and data retention limits should be tied to the original purposes for collecting the data. Consumers need to be informed about what data is being collected about their Internet activities, how the information will be used, whether the information will be shared with others, and what measures are being taken to ensure that any transfer of data remains secure. They should be presented with this information in a manner that supports informed choice over their information and that choice should honored persistently over time. Consumers must also have opportunities for legal redress for misuse of the data. As a recent D.C. District Court opinion established, data leakage and the concern for potential abuses of that data are recognizable harms standing alone, without any need to show misuse of the data.[9] Consumers do not need to become victims of identity theft to suffer from an invasion of privacy.

There is also a risk that profiles for behavioral advertising may be used for purposes other than advertising. For example, ad networks that focus on "re-targeting" ads may already be using profiles to help marketers engage in differential pricing.[10] Behavioral profiles, particularly those that can be tied to an individual, may also be a tempting source of information in making decisions about credit, insurance, and employment. While the lack of transparency makes it almost impossible to know whether behavioral profiles are being used for other purposes, the lack of enforceable rules around the collection and use of most personal information leaves the door wide open for a myriad of secondary uses.

Finally, because the legal standards for government access to personal information held by third parties are extraordinarily low, these comprehensive consumer profiles are available to government officials by mere subpoena, without notice to the individual or an opportunity for the individual to object.[11]

---

[9] *Am. Fed'n of Gov't Employees v. Hawley*, D.D.C., No. 07-00855, 3/31/08 (ruling, *inter alia*, that concerns about identity theft, embarrassment, inconvenience, and damage to financial suitability requirements after an apparent data breach constituted a recognizable "adverse effect" under the Privacy Act, 5 U.S.C. § 552(a) (citing *Kreiger v. Dep't of Justice*, 529 F.Supp.2d 29, 53 (D.D.C. 2008)).

[10] *See* Louise Story, "Online Pitches Made Just For You," *The New York Times* (Mar. 2008), http://www.nytimes.com/2008/03/06/business/media/06adco.html.

[11] *See* Center for Democracy & Technology, *Digital Search and Seizure: Updating Privacy Protections to Keep Pace with Technology* (2006), http://www.cdt.org/publications/digital-search-and-seizure.pdf at 7-9; Deirdre K. Mulligan, "Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act," 72 Geo. Wash. L. Rev. 1557 (Aug. 2004); Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy," 75 S. Cal. L. Rev. 1083, 1135 (2002).

IV. The Use of Sensitive Information for Behavioral Advertising

The concerns about behavioral advertising practices are heightened because of the increasingly sensitive nature of the information that consumers are providing online in order to take advantage of new services and applications. Two data types of particular concern are health information and location information.

A. Personal Health Information – Increasingly Available Online

Personal health data is migrating online through an ever-expanding array of health information and search sites, online support groups, and personal health record sites. Federal privacy rules under the Health Information Portability and Accountability Act ("HIPAA") do not cover personal health information once it moves online and out of the control of HIPAA-covered entities. Once it is posted online, it may have no more legal protection than any other piece of consumer information. In addition, information provided by consumers that is not part of a "medical record" – such as search terms – may nevertheless reveal highly sensitive information. We do not know the full extent to which personal health data is being collected for behavioral advertising. We do know that the limits placed on its collection by the industry are inadequate and that there is an urgent need to develop a definition for personal health information in the Internet context that is robust enough to protect privacy.

B. Location Information – Not Always Protected By Current Law

As technologies converge and Internet services are provided over cellular phones and other mobile devices, the ability to physically locate consumers is spurring location-based advertising, targeted to where a user is at any given moment. Plans to incorporate location information into behavioral advertising are still in development. Although laws exist to protect location information collected by telecommunications carriers, applications providers are increasingly offering location-based services that fall completely out of that legal framework. Standards for government access to location information are also unclear, even as law enforcement has shown a greater interest in such information.[12]

V. The Emerging Use of ISP Data for Behavioral Advertising

[12] *See* Center for Democracy & Technology, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology* (2006), http://www.cdt.org/publications/digital-search-and-seizure.pdf at 23-29.

The use of ISP data for behavioral advertising is one area that requires close scrutiny from lawmakers. The interception and sharing of Internet traffic content for behavioral advertising defies reasonable user expectations, can be disruptive to Internet and Web functionality, and may run afoul of communications privacy laws.

A. How ISP Data is Used for Behavioral Advertising

In this new model, an ad network strikes a deal with an ISP that allows the network to receive the contents of the individual Web traffic streams of each of the ISP's customers. The ad network analyzes the content of the traffic in order to create a record of the individual's online behaviors and interests. As customers of the ISP surf the Web and visit sites where the ad network has purchased ad space, they see advertisements targeted based on their previous Internet behavior. While the model as it exists today involves an ISP contracting with a third party that operates such an ad network, it would also be possible for ISPs to do the traffic content inspection, categorization, and advertising delivery themselves.

B. Privacy Implications of the Use of ISP Data for Behavioral Advertising

The privacy implications of behavioral advertising at large are amplified in this ISP model. Ad networks that partner with ISPs may potentially gain access to all or substantially all of an individual's Web traffic as it traverses the ISP's infrastructure, including traffic to all political, religious, and other non-commercial sites. While traditional ad networks may be large, few if any provide the opportunity to collect information about an individual's online activities as comprehensively as in the ISP model, particularly with respect to activities involving non-commercial content. And although these ad networks currently inspect predominantly Web traffic, ISPs carry emails, chats, file transfers and many other kinds of data that they could decide to pass on to behavioral ad networks in the future.

Moreover, the use of Internet traffic content for behavioral advertising defies user expectations about what happens when they surf the Web and communicate online. Absent unmistakable notice, consumers simply do not expect their ISP or its partners to be looking into the content of their Internet communications. Finding out that there is a middleman lurking between consumers and the Web sites they visit would come as a unwelcome surprise to most Internet users. ISPs are a critical part of the chain of trust that undergirds the Internet. Giving an unknown third party broad access to all or most consumer communications may undermine that trust.

C. Current Implementations May Interfere With Normal Internet Use

Despite these concerns, several ad network companies are moving forward with plans to use ISP data for behavioral advertising. The two most prominent ad networks engaged in this practice are NebuAd in the United States and Phorm in the UK. Charter Communications, a cable broadband ISP, recently announced – and then delayed – a plan to conduct trials of the NebuAd behavioral advertising technology.[13] Several other ISPs, such as Wide Open West (WOW!), CenturyTel, Embarq and Knology also announced plans with NebuAd to trial or deploy its behavioral advertising technology. Although a number of these ISPs have put their plans on hold in the wake of a firestorm of criticism, NebuAd continues to work with U.S. ISPs and seek new ISP partners. Phorm, which originally announced deals with three of the UK's largest ISPs and has sought partnerships with U.S. ISPs, is also now encountering hesitation from some of its partners.[14]

Independent analyses of both companies' systems have revealed that by virtue of their ability to intercept Internet traffic in the middle of the network – and based on their desire to track individual Internet users – they engage in an array of practices that are inconsistent with the usual flow of Internet traffic. NebuAd reportedly injects computer code into Web traffic streams that causes numerous cookies to be placed on users' computers for behavioral tracking, none of which are related to or sanctioned by the Web sites the users visit.[15] When a user navigates to a particular Web site, Phorm reportedly pretends to be that Web site so that it can plant a behavioral tracking cookie linked to that site on the user's computer.[16] In addition to the privacy implications of tracking all of an individual's Web activities, this kind of conduct has the potential to create serious security vulnerabilities in the network,[17] hamper the speed of users' Internet connections, and interfere with ordinary Web functionality. At a time when many different kinds of companies are working to build a trusted

---

[13] Saul Hansell, "Charter Suspends Plan to Sell Customer Data to Advertisers," *The New York Times: Bits Blog* (Jun. 2008), http://bits.blogs.nytimes.com/2008/06/24/charter-suspends-plan-to-sell-customer-data-to-advertisers/?scp=3-b&sq=charter+nebuad&st=nyt.

[14] Chris Williams, "CPW builds wall between customers and Phorm," *The Register* (Mar. 2008), http://www.theregister.co.uk/2008/03/11/phorm_shares_plummet/

[15] Robert M. Topolski, *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking*, Free Press and Public Knowledge (Jun 2008), http://www.publicknowledge.org/pdf/nebuad-report-20080618.pdf.

[16] Richard Clayton, *The Phorm "Webwise" System* (May 2008), http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf.

[17] These types of behaviors have much in common with well-understood online security threats, and parts of the Internet security community are already investigating how to respond. *See* Anti-Spyware Coalition, "Anti-Spyware Coalition Aims to Address Behavioral Targeting" (Apr. 2008), http://antispywarecoalition.org/newsroom/20080425press.htm.

computing platform for the Internet, having ISPs work with partners whose practices undermine trust raises future cyber-security concerns.

D. Current Implementations May Violate Federal Law

Depending on how this advertising model is implemented, it may also run afoul of existing communications privacy laws. The federal Wiretap Act, as amended by the Electronic Communications Privacy Act ("ECPA"), prohibits the interception and disclosure of electronic communications – including Internet traffic content – without consent.[18] Although exceptions to this rule permit interception and disclosure without consent, we seriously doubt that any of them apply to the interception or disclosure of Internet traffic content for behavioral advertising purposes. Accordingly, we believe that the Wiretap Act requires unavoidable notice and affirmative opt-in consent before Internet traffic content may be used from ISPs for behavioral advertising purposes. Certain state laws may take this one step further, requiring consent from both parties to the communication: the consumer and the Web site he or she is visiting. A detailed CDT legal memorandum on the application of the Wiretap Act, ECPA and relevant state wiretap laws to the use of ISP data for behavioral advertising is attached as Appendix B.

As several members of Congress have noted, the Cable Communications Policy Act also applies here.[19] The law prohibits cable operators from collecting or disclosing personally identifiable information without prior consent.[20] While the term "personally identifiable information" in the law is defined by what it does not include – "any record of aggregate data which does not identify particular persons"[21] – we doubt that a user's entire Web traffic stream, unique to that individual, often containing both PII and non-PII, would be considered aggregate data as that term is commonly understood.

We do not believe that it is possible to shoehorn the collection and disclosure of a subscriber's entire browsing history for advertising purposes into the statute's exception for collection or disclosure of information that is necessary to render

---

[18] 18 U.S.C. § 2511.

[19] House Representative Edward Markey and House Representative Joe Barton, *Letter to Charter Communications CEO in Regards to the Charter-NebuAd Data Collection Scheme* (May 2008) http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf. A 1992 amendment adding the phrase "other services" to the Cable Act's privacy provision made it clear that the law covers Internet services provided by cable operators.

[20] 47 U.S.C. § 551(b)-(c).

[21] *Id.* § 551(a)(2)(A).

service.[22] Thus, we conclude that cable-based ISPs that wish to disclose customer information to advertising networks would also have to meet the consent requirements of the Cable Communications Policy Act.

The ISP models that have been deployed thus far have failed to obtain affirmative, express opt-in consent required by law. Several small U.S. ISPs, for example, have failed to meet this threshold requirement, burying vague information about their deals with NebuAd in the ISPs' terms of service.[23] Charter Communications, the largest U.S. ISP that had planned to partner with NebuAd, notified its subscribers that they would be receiving more relevant ads, but did not explain its plans to intercept subscribers' traffic data, and did not provide a way for subscribers to give or withhold consent. Charter has since suspended its plans.

Designing a robust opt-in consent system for ISP-based behavioral advertising presents a formidable challenge. We are less than sanguine that such a system can be easily designed, particularly since it must not only provide a way for consumers to give affirmative consent, but it must also provide a method for them to revoke that consent. The burden is on those who wish to move forward with the model to demonstrate that an express notice and consent regime can work in this context.

VI. The Limits of Self-Regulation

For almost a decade, the primary privacy framework for the behavioral advertising industry has been provided by the Network Advertising Initiative, a self-regulatory group of online advertising networks formed in response to pressure from the Federal Trade Commission and consumer advocates in the wake of privacy concerns over the merger of ad network DoubleClick and Abacus, an offline data broker. NAI members agree to provide consumers with notice and, at minimum, a method to opt out of behavioral advertising. They further pledged to use information collected for only for marketing purposes. While at the time of their release CDT welcomed the NAI principles as an important first step, we also noted then that there were flaws in the approach that needed to be addressed and that self-regulation was not a complete solution. The FTC agreed, concluding in its July 2000 report to Congress that "backstop

[22] *Id.* § 551(a)(2)(B).

[23] *See* Mike Masnick, "Where's The Line Between Personalized Advertising And Creeping People Out?," *TechDirt* (Mar. 2008), http://www.techdirt.com/articles/20080311/121305499.shtml; Peter Whoriskey, "Every Click You Make," *The Washington Post* (Apr. 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule.

legislation addressing online profiling is still required to fully ensure that consumers' privacy is protected online."[24] That remains true today.

Eight years after the creation of the principles, few consumers are aware of behavioral advertising and fewer still have been able to successfully navigate the confusing and complex opt-out process.[25] Although individual NAI companies have launched their own consumer awareness initiatives, more work remains to be done.[26] For those consumers who successfully opt out, the NAI's reliance on flawed opt-out cookies means that user preferences are often not persistently honored.

In addition, the NAI's guidelines for the use of sensitive information have never been adequate to guard consumer privacy. Until recently, the definition was limited to a narrowly defined set of PII. While the definition is being revised, it still falls far short of what is needed to address the increasingly sensitive nature of consumer information online.[27]

Finally, the NAI principles only apply to companies that voluntarily join the initiative. The NAI has no way to force companies to join; the current membership is missing numerous behavioral advertising firms, including some key industry players. In addition, measures to ensure compliance and transparency have withered on the vine.[28] The original NAI principles provided

---

[24] Federal Trade Commission, *Online Profiling: A Report to Congress* (Jul. 2000), http://www.ftc.gov/os/2000/07/onlineprofiling.htm.

[25] The drawbacks of opt-out cookies have been well documented: they are confusing for the majority of consumers who do not understand the technology and counter-intuitive to those who are accustomed to deleting their cookies to protect their privacy. Cookies are susceptible to accidental deletion and file corruption. While the NAI is in the process of updating the principles, it has not proposed changes to the opt-out regime. *See* Center for Democracy & Technology, *Applying the FTC's Spyware Principles to Behavioral Advertising: Comments of the Center for Democracy & Technology in regards to the FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology*" (Oct. 2007), http://www.cdt.org/privacy/20071019CDTcomments.pdf at 8.

[26] *See, e.g.,* AOL, *Mr. Penguin* (last visited Jul. 2008), http://corp.aol.com/o/mr-penguin/; Yahoo!, *Customized Advertising* (last visited Jul. 2008), http://info.yahoo.com/relevantads/; Google, *The Google Privacy Channel* (last visited Jul. 2008), http://youtube.com/user/googleprivacy.

[27] Center for Democracy & Technology, *Comments Regarding the NAI Principles 2008: The Network Advertising Initiative's Self-Regulatory Code of Conduct for Online Behavioral Advertising* (June 2008), http://www.cdt.org/privacy/20080612_NAI_comments.pdf at 6-9.

[28] CDT testing has revealed that only a tiny fraction of companies that collect data that could be used for behavioral advertising are NAI members. *See* Center for Democracy & Technology, *Statement of The Center for Democracy & Technology before The Antitrust, Competition Policy and Consumer Rights Subcommittee of the Senate Committee on the Judiciary on "An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What Are the Risks for Competition and Privacy?"* (Sept. 2007), http://www.cdt.org/privacy/20070927committee-statement.pdf.

for independent audits and enforcement against non-compliant members, but the audit results were never made public, and reporting on compliance with the principles has been inconsistent.[29]

For all these reasons, while we encourage more robust self-regulatory efforts, we continue to have doubts about the effectiveness of the self-regulatory framework. As online advertising becomes increasingly complex and data collection becomes more pervasive, Congress and the FTC must step in to ensure that consumer interests are fully protected.

VII. The Role of Congress

Congress should take action to address the significant privacy concerns raised by behavioral advertising:

- As a first step, we urge the Committee to hold a series of hearings to examine specific aspects of behavioral advertising. In particular, we believe that further investigation of new models of behavioral advertising using ISP data is warranted, and that the Committee should explore how current laws such as ECPA, the Wiretap Act and the Cable Communications Policy Act apply. Secondary uses of behavioral advertising profiles for purposes other than marketing also deserve additional investigation and scrutiny, as does the use of sensitive information.
- This Committee should set a goal of enacting in the next year general privacy legislation covering both the online and offline worlds. CDT has long argued for simple, flexible baseline consumer privacy legislation that would protect consumers from inappropriate collection and misuse of their personal information while enabling legitimate business use to promote economic and social value. In principle, such legislation would codify the fundamentals of fair information practices, requiring transparency and notice of data collection practices, providing consumers with meaningful choice regarding the use and disclosure of that information, allowing consumers reasonable access to personal information they have provided, providing remedies for misuse or unauthorized access, and setting standards to limit data collection and ensure data security.
- The Federal Trade Commission has played a helpful role in consumer education efforts around behavioral advertising. But it also must exercise its authority under its deception and unfairness jurisdiction to issue

[29] *See* Pam Dixon, *The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation* (Nov. 2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf at 16-17.

enforceable guidelines for behavioral advertising. We ask the Committee to strongly urge the Commission to exercise the full measure of its enforcement authority over online advertising practices.

- Congress should also examine and strengthen existing communications privacy laws to cover new services, technologies and business models with consistent rules. ECPA was passed more than 20 years ago, long before there was a World Wide Web and the Internet became integrated into Americans' daily lives. The application of the law to common online activities including Web search remains unclear and the legal protections it provides for the enormous amounts of personal data stored online are far too low.
- Finally, Congress should encourage the FTC to investigate how technology can be harnessed to give consumers better control over their online information. The lack of effective controls and the difficulty that consumers have in exercising choice about their participation in online tracking and targeting was the motivation behind the "Do Not Track" list idea proposed by CDT and nine other consumer and privacy groups.[30] Although the proposal has been controversial, the idea behind Do Not Track is both simple and important: provide consumers with an easy-to-use, technology-neutral, persistent way to opt out of behavioral advertising. Congress should promote further study of this idea and other innovative ways to put consumers in control of their information.

VIII. Conclusion

I would like to thank the Committee again for holding this important hearing. We believe that Congress has a critical role to play in ensuring that privacy is protected in an increasingly complex online advertising environment. CDT looks forward to working with the Committee as it pursues these issues further.

[30] *See* Pam Dixon et al, *Consumer Rights and Protections in the Behavioral Advertising Sector* (Oct. 2007), http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.

Appendix A:

Simplified Illustration of a Traditional Online Ad Network

Figure 1 below shows a simplified version of a traditional online ad network. Ad networks contract with advertisers on one side and publishers on the other. They take the ads they receive from advertisers and match them to open ad spaces on publisher sites.

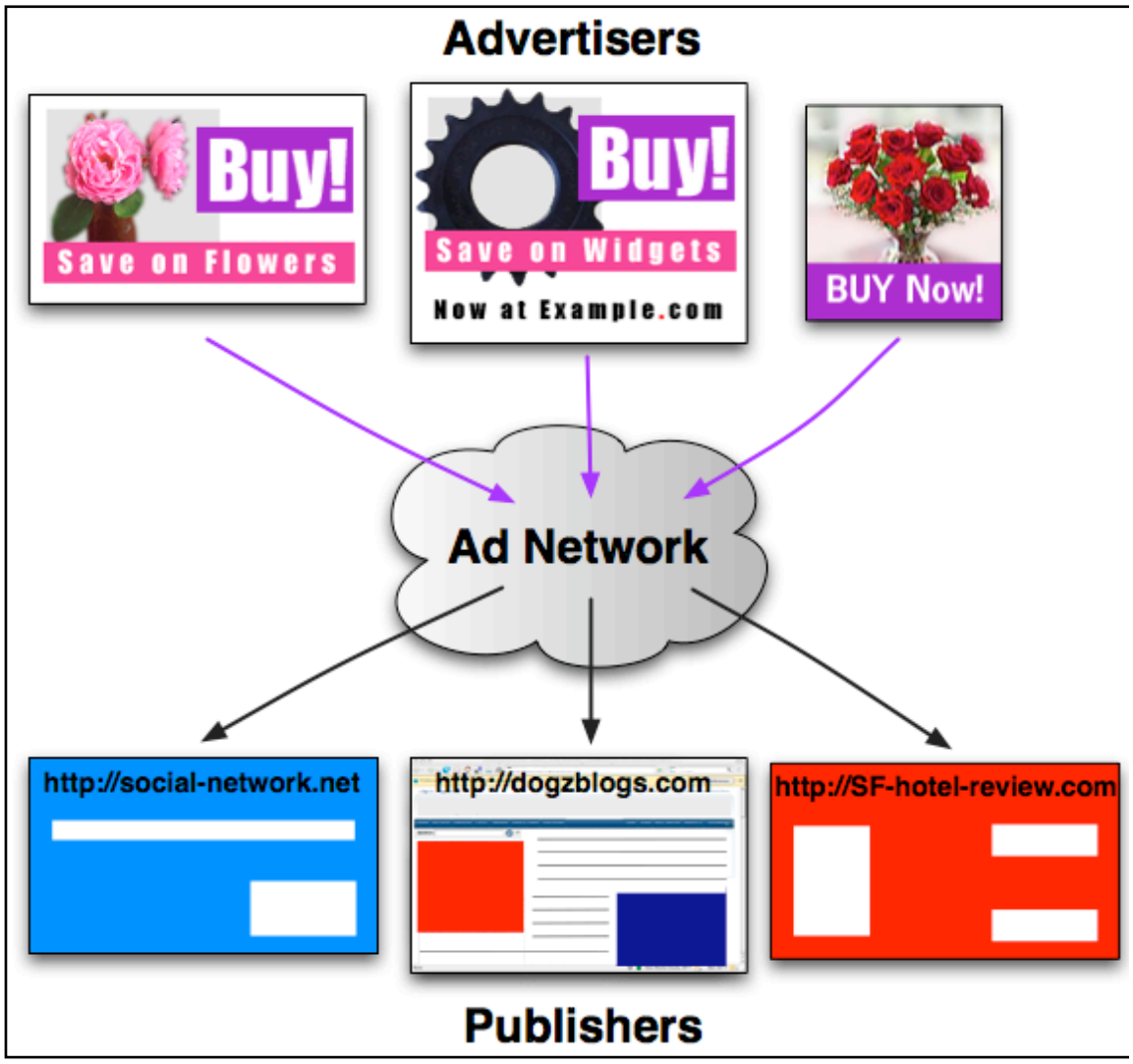

Figure 1.

Figure 2 shows how an ad network collects data about a consumer's Web activities. When the consumer first visits a publisher site in the network (SF-hotel-review.com), the ad network places a cookie with a unique ID (12345) on the consumer's computer. When the user subsequently visits other publisher sites in the network (including dogzblogs.com and social-network.net), the cookie containing the ID is automatically transmitted to the ad network. This allows the ad network to keep track of what sites the consumer has visited and build a behavioral profile based on that information, linked to the cookie ID.

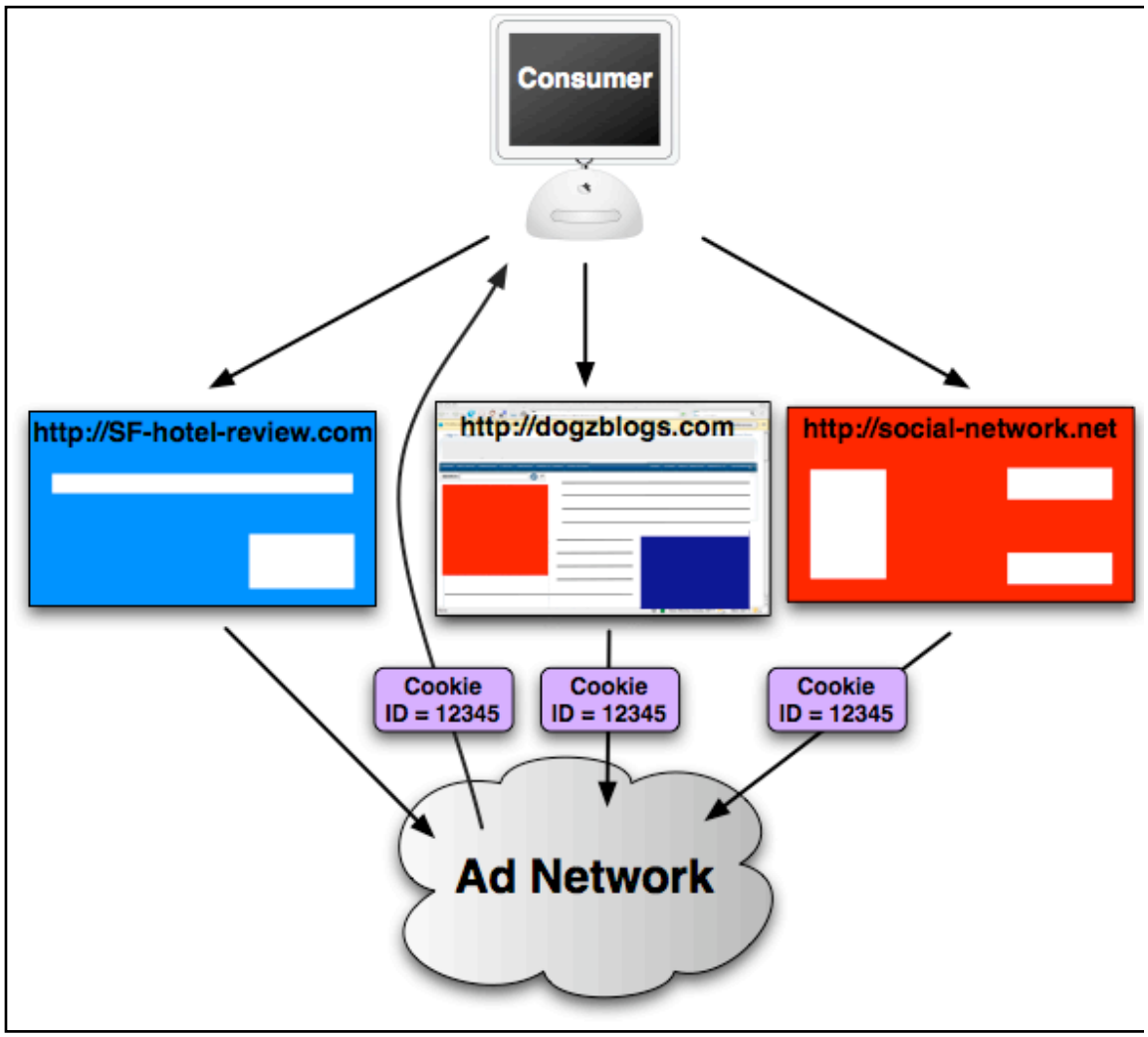

Figure 2

Appendix B:

An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising

July 8th, 2008

Much of the content on the Internet (just like content in newspapers, broadcast TV, radio and cable) is supported in whole or part by advertising revenue. The Internet offers special opportunities to target ads based on the expressed or inferred interests of the individual user. There are various models for delivering targeted ads online. These range from the purely contextual (everyone who visits a travel site sees the same airline ad) to models that involve compiling information about the online behavior of individual Internet users, to be used in serving them advertisements. For years, Web sites have entered into agreements with advertising networks to use "cookies" to track individual users across Web sites in order to compile profiles. This approach has always been, and remains, a source of privacy concern, in part because the conduct usually occurs unbeknownst to most Internet users. Recent developments, including the mergers between online service providers and some of the largest online advertising networks, have heightened these concerns. The Center for Democracy & Technology has been conducting a major project on behavioral advertising, in which we have been researching behavioral advertising practices, consulting with Internet companies and privacy advocates, developing policy proposals, filing extensive comments at the FTC, and analyzing industry self-regulatory guidelines.

This memo focuses on the implications of a specific approach to behavioral advertising being considered by Internet advertising networks and Internet Service Providers (ISPs). This new approach involves copying and inspecting the content of each individual's Internet activity with the cooperation of his or her ISP.[31] Under this new model, an advertising network strikes a deal with an

[31] *See, e.g.,* Peter Whoriskey, *Every Click You Make*, WASH. POST (Apr. 3, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule; Saul Hansell, *I.S.P. Tracking: The Mother of All Privacy Battles*, N.Y. TIMES: BITS BLOG (Mar. 20, 2008), http://bits.blogs.nytimes.com/2008/03/20/isp-tracking-the-mother-of-all-privacy-battles/?scp=1-b&sq=the+mother+of+all+privacy+battles&st=nyt.

ISP, and the ISP allows the network to copy the contents of the individual Web traffic streams of each of the ISP's customers. The advertising network analyzes the content of these traffic streams in order to create a record of each individual's online behaviors and interests. Later, as customers of the ISP surf the Web and visit sites where the advertising network has purchased advertising space, they see ads targeted based on their previous Internet behavior.

NebuAd is one such advertising network company operating in the United States. In the past few months, it has come to light that NebuAd was planning to partner with Charter Communications, a cable broadband ISP, to conduct trials of the NebuAd behavioral advertising technology. Several other smaller ISPs, such as Wide Open West (WOW!), CenturyTel, Embarq, and Knology, have also announced plans with NebuAd to trial or deploy its behavioral advertising technology. In response to concerns raised by subscribers, privacy advocates, and policymakers, Charter, CenturyTel and Embarq have delayed these plans, but NebuAd and other similar companies are continuing to seek new ISP partners.

The use of Internet traffic content from ISPs for behavioral advertising is different from the "cookie"-based model in significant ways and raises unique concerns.[32] Among other differences, it copies all or substantially all Web transactions, including visits to sites that do not use cookies. Thus, it may capture not only commercial activity, but also visits to political, advocacy, or religious sites or other non-commercial sites that do not use cookies.

In this memo, we conclude that the use of Internet traffic content from ISPs may run afoul of federal wiretap laws unless the activity is conducted with the consent of the subscriber.[33] To be effective, such consent should not be buried in terms of service and should not be inferred from a mailed notice. We recommend prior, express consent, but we do not offer here any detailed recommendations on how to obtain such consent in an ISP context. Also, we note that that the California law requiring consent of all the parties to a communication has been applied by the state Supreme Court to the monitoring

---

[32] Privacy concerns also apply to advertising-based models that have been developed for services, such as email, that ride over ISP networks. *See* CDT Policy Post 10.6, *Google GMail Highlights General Privacy Concerns* (Apr. 12, 2004), http://www.cdt.org/publications/policyposts/2004/6 (recommending express prior opt-in for advertising-based email service).

[33] Additional questions have been raised under the Cable Communications Policy Act. *See* Rep. Edward Markey and Rep. Joe Barton, *Letter to Charter Communications CEO in Regards to the Charter-NebuAd Data Collection Scheme* (May 2008), http://markey.house.gov/docs/telecomm/letter_charter_comm_privacy.pdf. In this memo, we focus on issues arising under the federal Wiretap Act, as amended by the Electronic Communications Privacy Act.

of telephone calls when the monitoring is done at a facility outside California. The California law so far has not been applied to Internet communications and it is unclear whether it would apply specifically to the copying of communications as conducted for behavioral monitoring purposes, but if it or another state's all-party consent rule were applied to use of Internet traffic for behavioral profiling, it would seem to pose an insurmountable barrier to the practice.

Wiretap Act

A. Service Providers Cannot "Divulge" The Contents of Subscriber Communications, Except Pursuant to Limited Exceptions

The federal Wiretap Act, as amended by the Electronic Communications Privacy Act, protects the privacy of wire, oral, and electronic communications.[34] "[E]lectronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . ."[35] Web browsing and other Internet communications are clearly electronic communications protected by the Wiretap Act.

In language pertinent to the model under consideration, § 2511(3) of the Act states that "a person or entity providing an electronic communication service to the pubic shall not intentionally divulge the contents of any communications . . . while in transmission on that service to any person or entity other than an addressee or intended recipient . . . ."[36]

There are exceptions to this prohibition on disclosure, two of which may be relevant here. One exception specifies that "[i]t shall not be unlawful under this chapter for an . . . electronic communication service, whose facilities are used in the transmission of a[n] . . . electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a *necessary incident to the rendition of his service* or to the

[34] 18 U.S.C. §§ 2510-2522.

[35] *Id.* § 2510(12).

[36] *Id.* § 2511(3)(a). Lest there be any argument that the disclosure does not occur while the communications are "in transmission," we note that the Stored Communications Act (SCA) states that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." *Id.* § 2702(a)(1). We do not comment further here on the SCA because, in our judgment, the approach that has been described so far clearly involves the divulging of communications "while in transmission."

protection of the rights or property of the provider of that service."[37] We will refer to this as the "necessary incident" exception. The second exception is for disclosures with the consent of one of the parties.[38] We will discuss both exceptions below. We conclude that only the consent exception applies to the disclosure of subscriber content for behavioral advertising, and we will discuss preliminarily what "consent" would mean in this context.

B. With Limited Exceptions, Interception Is Also Prohibited

The Wiretap Act regulates the "interception" of electronic communications. The Act defines "intercept" as the "acquisition of the contents of any … electronic … communication through the use of any electronic, mechanical, or other device."[39]

The Wiretap Act broadly bars all intentional interception of electronic communications.[40] The Act enumerates specific exceptions to this prohibition.[41] Law enforcement officers, for example, are authorized to conduct interceptions pursuant to a court order. For ISPs and other service providers, there are three exceptions that might be relevant. Two we have mentioned already: the "necessary incident" exception and a consent exception.[42]

A third exception, applicable to interception but not to disclosure, arises from the definition of "intercept," which is defined as acquisition by an "electronic, mechanical, or other device," which in turn is defined as "any device or apparatus which can be used to intercept a[n] . . . electronic communication *other than*—(a) any telephone or telegraph instrument, equipment or facility, or any component thereof . . . (ii) being used by a provider of . . . electronic communication service in the *ordinary course of its business* . . . ."[43] This provision thus serves to limit the definition of "intercept," providing what is sometimes called the "telephone extension" exception, but which we will call the "business use" exception.

---

[37] *Id.* § 2511(2)(a)(i) (emphasis added). This analysis focuses on the capture of electronic communications and definitions are abridged accordingly.

[38] *Id.* § 2511(3)(b)(ii).

[39] *Id.* § 2510(4).

[40] *Id.* § 2511(1).

[41] *Id.* § 2511(2).

[42] Separate from the consent provision for disclosure, the consent exception for interception is set forth in 18 U.S.C. § 2511(2)(d): "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a[n] . . . electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception . . . ."

[43] *Id.* § 2510(5) (emphasis added).

C. The Copying of Internet Content for Disclosure to Advertising Networks Constitutes Interception

When an ISP copies a customer's communications or allows them to be copied by an advertising network, those communications have undoubtedly been "intercept[ed]."[44] Therefore, unless an exception applies, it seems likely that placing a device on an ISP's network and using it to copy communications for use in developing advertising profiles would constitute illegal interception under § 2511(1)(a); similarly, the disclosure or use of the intercepted communications would run afoul of § 2511(1)(c) or § 2511(1)(d), respectively.

D. The "Necessary Incident" Exception Probably Does Not Permit the Interception or Disclosure of Communications for Behavioral Advertising Purposes

The Wiretap Act permits interception of electronic communications when the activity takes place as "a necessary incident to the rendition of [the ISP's] service or to the protection of the rights or property of the provider of that service."[45] The latter prong covers anti-spam and anti-virus monitoring and filtering and various anti-fraud activities, but cannot be extended to advertising activities, which, while they may enhance the service provider's revenue, do not "protect" its rights. Courts have construed the "necessary incident" prong quite strictly, requiring a service provider to show that it *must* engage in the activity in order to carry out its business.[46] It is unlikely that the copying, diversion, or disclosure of Internet traffic content for behavioral advertising would be construed as a "necessary incident" to an ISP's business. Conceivably, an ISP could argue that its business included copying its subscribers communications and providing them to third parties for purposes of placing advertisements on Web sites unaffiliated with the ISP, but the ISP would probably have to state that that business existed and get the express agreement of its customers that they were

---

[44] *See, e.g.,* United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) (holding in context of telephone communications that "when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time" and that "[r]edirection presupposes interception"); *In re* State Police Litig., 888 F. Supp. 1235, 1267 (D. Conn. 1995) (stating in context of telephone communications that "it is the act of diverting, and not the act of listening, that constitutes an 'interception'").

[45] 18 U.S.C. § 2511(2)(a)(i).

[46] *See* United States v. Councilman, 418 F.3d 67, 82 (1st Cir. 2005) (en banc) (holding that service provider's capture of emails to gain commercial advantage "clearly" was not within service provider exception); Berry v. Funk, 146 F.3d 1003, 1010 (D.C. Cir. 1998) (holding in context of telephone communications that switchboard operators' overhearing of a few moments of phone call to ensure call went through is a "necessary incident," but anything more is outside service provider exception).

subscribing to that business as well as the basic business of Internet access, which leads anyhow to the consent model that we conclude is necessary.

E. While It Is Unclear Whether the "Business Use" Exception Would Apply to the Use of a Device Installed or Controlled by a Party Other than the Service Provider, the Exception Does Not Apply to the Prohibition Against Divulging a Subscriber's Communications

The "business use" exception, § 2510(5)(a), constricts the definition of "device" and thereby narrows the definition of "intercept" in the Wiretap Act. There are two questions involved in assessing applicability of this exception to the use of Internet traffic content for behavioral advertising: (1) whether the device that copies the content for delivery to the advertising network constitutes a "telephone or telegraph instrument, equipment or facility, or any component thereof," and (2) whether an ISP's use of the device would be within the "ordinary course of its business."

We will discuss the "business use" exception at some length, because there has been considerable discussion already about whether copying of an ISP subscriber's communications for behavioral advertising is an "interception" under § 2511(1) of the Wiretap Act. However, even if the business use exception applied, an ISP would only avoid liability for the *interception* of electronic communications. It would still be prohibited from divulging the communications of its customers to an advertising network under the separate section of the Wiretap Act, § 2511(3), which states that a service provider "shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient . . . ."[47] The business use exception does not apply to this prohibition against divulging.[48]

At first glance, it would seem that the business use exception is inapplicable to the facilities of an ISP because the exception applies only to a "telephone or telegraph instrument, equipment or facility, or any component thereof." However, the courts have recognized that ECPA was motivated in part by the

---

[47] 18 U.S.C. § 2511(3)(a).

[48] By adopting two different exceptions—"necessary incident" and "ordinary course"—Congress apparently meant them to have different meanings. Based on our reading of the cases, the necessary incident exception is narrower than the ordinary course exception. It is significant that the "necessary incident" exception applies to both interception and disclosure while the "ordinary course" exception is applicable only to interception. This suggests that Congress meant to allow service providers broader latitude in examining (that is, "intercepting" or "using") subscriber communications so long as they did not disclose the communications to third parties. This permits providers to conduct a range of in-house maintenance and service quality functions that do not involve disclosing communications to third parties.

"dramatic changes in new computer and telecommunications technologies"[49] and therefore was intended to make the Wiretap Act largely neutral with respect to its treatment of various communications technologies. The Second Circuit, for example, concluded in a related context that the term "telephone" should broadly include the "instruments, equipment and facilities that ISPs use to transmit e-mail."[50] Therefore, as a general matter, it should be assumed that the business use exception is available to ISPs.

However, it is not certain that the device used to copy and divert content for behavioral advertising would be considered to be a component of the service provider's equipment or facilities. In some of the behavioral advertising implementations that have been described, the monitoring device or process is not developed or controlled by the ISP but rather by the advertising network.

The second question is whether an ISP's use of a device to copy traffic content for behavioral advertising falls within the "ordinary course of its business." There are a number of cases interpreting this exception, but none of them clearly addresses a situation where a service provider is copying all of the communications of its customers. Many of the cases arise in situations where employers are monitoring the calls of their employees for purposes of supervision and quality assurance. "These cases have narrowly construed the phrase 'ordinary course of business.'"[51] Often such cases also involve notice to the employees and implied consent.[52] One court has stated that, even if an entity could satisfy the business use exception, notice to one of the parties being monitored would be required.[53] Other cases involve the monitoring of prisoners.

Some cases have interpreted "ordinary course" to mean anything that is used in "normal" operations. The D.C. Circuit, for instance, has suggested that monitoring "undertaken normally" qualifies as being within the "ordinary course of business."[54] In the context of law enforcement taping of the phone calls of prisoners, the Ninth and Tenth Circuits have concluded that something is in the "ordinary course" if it is done routinely and consistently.[55] It might be that

---

[49] S. Rep. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

[50] Hall v. Earthlink Network, Inc., 396 F.3d 500, 505 (2d Cir. 2005) (quoting S. Rep. No. 99-541 at 8).

[51] United States v. Murdock, 63 F.3d 1391. 1396 (6th Cir 1995).

[52] *E.g.,* James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979).

[53] *See, e.g.,* Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001).

[54] Berry v. Funk, 146 F.3d 1003, 1009 (D.C. Cir. 1998) (workplace monitoring).

[55] *See* United States v. Van Poyck, 77 F.3d 285, 292 (9th Cir. 1996); United States v. Gangi, 57 Fed. Appx. 809, 814 (10th Cir. 2003).

courts would give equal or greater latitude to service providers in monitoring their networks than they would give to mere subscribers or users.

Other circuit courts have used a more limited interpretation, concluding that "ordinary course" only applies if the device is being used to intercept communications for "legitimate business reasons."[56] Although the courts have not been entirely clear as to what that means, some have suggested that it is much closer to necessity than to mere profit motive.[57] One frequently-cited case explicitly holds that the business use exception does not broadly encompass a company's financial or other motivations: "The phrase 'in the ordinary course of business' cannot be expanded to mean anything that interests a company."[58]

Normal principles of statutory interpretation would require that some independent weight be given to the word "ordinary," so that the exception does not encompass anything done for business purposes. It is unclear, however, how much weight courts would give to the word "ordinary" in a rapidly changing market. It does not seem that the phrase "ordinary course of business" should preclude innovation, but courts might refer to past practices and normal expectations surrounding a line of business and specifically might look to what customers have come to expect.

Viewed one way, it is hard to see how the copying of content for behavioral advertising is part of the "ordinary course of business" of an ISP. After all, the ISP is not the one that will be using the content to develop profiles of its customers; the profiling is done by the advertising network, which does not even disclose to the ISP the profiles of its own subscribers. (The profiles are proprietary to the advertising network and it is careful not to disclose them to anyone.) Very few (if any) of the ads that are placed using the profiles will be ads for the ISP's services; they will be ads for products and services completely unrelated to the ISP's "ordinary course of business." Moreover, the ads will be

---

[56] *See* Arias v. Mutual Central Alarm Serv., Inc., 202 F.3d 553, 560 (2d Cir. 2000) (monitoring calls to an central alarm monitoring service).

[57] *See id.* (concluding that alarm company had legitimate reasons to tap all calls because such businesses "are the repositories of extremely sensitive security information, including information that could facilitate access to their customers' premises"); *see also* First v. Stark County Bd. of Comm'rs, 234 F.3d 1268, at *4 (6th Cir. 2000) (table disposition).

[58] Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983). Watkins states: "We hold that a personal call may not be intercepted in the ordinary course of business under the exemption in section 2510(5)(a)(i), except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents." 704 F.2d at 583. This language supports the conclusion that the business use exception could not cover wholesale interception of ISP traffic, no more than switchboard operators can perform wholesale monitoring of telephone traffic.

placed on Web sites having no affiliation with the ISP. On the other hand, the ISP could argue that part of its business model—part of what keeps its rates low—is deriving revenue from its partnership with advertising networks.

The legislative histories of the Wiretap Act and ECPA weigh against a broad reading of the business use exception. Through these laws, Congress intended to create a statutory regime generally affording strong protection to electronic communications. Congress included limited, specific and detailed exceptions for law enforcement access to communications, and other limited, specific and detailed exceptions to allow companies providing electronic communications service to conduct ordinary system maintenance and operational activities. Congress gave especially high protection to communications content. If the business use exception can apply any time an ISP identifies a new revenue stream that can be tapped though use of its customers' communications, this careful statutory scheme would be seriously undermined.

F. The Consent Exception: The Context Weighs Heavily in Favor of Affirmative, Opt-In Consent from ISP Subscribers

Consent is an explicit exception both to the prohibition against intercepting electronic communications under the Wiretap Act and to the Act's prohibition against disclosing subscriber communications. The key question is: How should consent be obtained for use of Internet traffic content for behavioral advertising? Courts have held in telephone monitoring cases under the Wiretap Act that consent can be implied, but there are relatively few cases specifically addressing consent and electronic communications. However, in cases involving telephone monitoring, one circuit court has stated that consent under the Wiretap Act "is not to be cavalierly implied."[59] Another circuit court has noted that consent "should not casually be inferred"[60] and that consent must be "actual," not "constructive."[61] Yet another circuit court has stated: "Without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception."[62] Furthermore, "knowledge of the *capability* of monitoring alone cannot be

[59] Watkins. 704 F.2d at 581 ("Consent under title III is not to be cavalierly implied. Title III expresses a strong purpose to protect individual privacy by strictly limiting the occasions on which interception may lawfully take place.").

[60] Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990).

[61] *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 20 (1st Cir. 2003); *see also* United States v. Corona-Chavez, 328 F.3d 974, 978 (8th Cir. 2003).

[62] Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (internal quotation omitted).

considered implied consent."[63] The cases where consent has been implied involve very explicit notice; many of them involve the monitoring of prisoners' phone calls.[64]

Consent is context-based. It is one thing to imply consent in the context of a prison or a workplace, where notice may be presented as part of the daily log-in process. It is quite another to imply it in the context of ordinary Internet usage by residential subscribers, who, by definition, are using the service for personal and often highly sensitive communications. Continued use of a service after a mailed notice might not be enough to constitute consent. Certainly, mailing notification to the bill payer is probably insufficient to put all members of the household who share the Internet connection on notice.

Thus, it seems that an assertion of implied consent, whether or not users are provided an opportunity to opt out of the system, would most likely not satisfy the consent exception for the type of interception or disclosure under consideration here. Express prior consent (opt-in consent) is clearly preferable and may be required. While meaningful opt-in consent would be sufficient, courts would likely be skeptical of an opt-in consisting merely of a click-through agreement—i.e., a set of terms that a user agrees to by clicking an on-screen button—if it displays characteristics typical of such agreements, such as a large amount of text displayed in a small box, no requirement that the user scroll through the entire agreement, or the opt-in provision buried among other terms of service.[65]

In regards to consent, the model under discussion here is distinguishable from the use of "cookies," which were found to be permissible by a federal district court in a 2001 case involving DoubleClick.[66] In that case, the Web sites participating in the DoubleClick advertising network were found to be parties to

---

[63] Watkins, 704 F.2d at 581; *see also* Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (holding that consent not implied when individual is aware only that monitoring might occur, rather than knowing monitoring is occurring).

[64] "The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of Title III-a purpose which suggests that consent should not casually be inferred." Griggs-Ryan, 904 F.2d at 117.

[65] *See, e.g.,* Specht v. Netscape Commc'ns Corp., 306 F.3d 17 (2d Cir. 2002) (rejecting online arbitration agreement because, among other things, site permitted customer to download product without having scrolled down to arbitration clause and agreement button said only "Download"); United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995) ("Deficient notice will almost always defeat a claim of implied consent.").

[66] *In re* DoubleClick Inc. Privacy Litig., 154 F.Supp.2d 497 (S.D.N.Y. 2001).

the communications of the Internet users who visited those sites. As parties to the communications, the Web sites could consent to the use of the cookies to collect information about those communications. Here, of course, the ISPs are not parties to the communications being monitored and the interception or disclosure encompasses communications with sites that are not members of the advertising network. Therefore, the source of consent must be the ISP's individual subscribers, as it would be impossible to obtain consent from every single Web site that every subscriber may conceivably visit.

State Laws Requiring Two-Party Consent to Interception

A. Summary

In addition to the federal Wiretap Act, a majority of states have their own wiretap laws, which can be more stringent than the federal law. Most significantly, twelve states[67] require all parties to consent to the interception or recording of certain types of communications when such interception is done by a private party not under the color of law.

In several of these states—for example, Connecticut—the all-party consent requirement applies only to the recording of oral conversations. In others, the all-party consent rule extends to both voice and data communications. For example, Florida's Security of Communications Act makes it a felony for any individual to intercept, disclose, or use any wire, oral, or electronic communication, unless that person has obtained the prior consent of all parties.[68] Similarly, the Illinois statute on criminal eavesdropping prohibits a person from "intercept[ing], retain[ing], or transcrib[ing an] electronic communication unless he does so . . . with the consent of all of the parties to such . . . electronic communication."[69]

The most important all-party consent law may be California's, because the California Supreme Court held in 2006 that the law can be applied to activity occurring outside the state.

[67] The twelve states are California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington.

[68] Fla. Stat. § 934.03(1).

[69] Ill. Comp Stat. 5/14-1(a)(1).

B. California

The 1967 California Invasion of Privacy Act makes criminally liable any individual who "intentionally taps, or makes any unauthorized connection . . . or who willfully and without the consent of all parties to the communication . . . reads, or attempts to read, or to learn the contents or meaning of any message . . . or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place" in California.[70] It also establishes liability for any individual "who uses, or attempts to use, in any manner . . . any information so obtained" or who aids any person in doing the same.[71] The law has a separate section creating liability for any person eavesdropping upon or recording a confidential communication "intentionally and without the consent of all parties," whether the parties are present in the same location or communicating over telegraph, telephone, or other device (except a radio).[72]

Consent can be implied only in very limited circumstances. The California state Court of Appeals held in *People v. Garber* that a subscriber to a telephone system is deemed to have consented to the telephone company's monitoring of his calls if he uses the system in a manner that reasonably justifies the company's belief that he is violating his subscription rights, and even then the company may only monitor his calls to the extent necessary for the investigation.[73] An individual can maintain an objectively reasonable expectation of privacy by explicitly withholding consent for a tape recording, even if the other party has indicated an intention to record the communication.[74]

In *Kearney v. Salomon Smith Barney, Inc.*, the state Supreme Court addressed the conflict between the California all-party consent standard and Georgia's wiretap law, which is modeled after the federal one-party standard.[75] It held that, where a Georgia firm recorded calls made from its Georgia office to residents in California, the California law applied. The court said that it would be unfair to impose damages on the Georgia firm, but prospectively the case effectively required out-of-state firms having telephone communications with people in California to announce to all parties at the outset their intent to record a

[70] Cal. Pen. Code § 631(a).

[71] *Id.*

[72] *Id.* § 632(a). The statute explicitly excludes radio communications from the category of confidential communications.

[73] 275 Cal. App. 2d 119 (Cal. App. 1st Dist. 1969).

[74] Nissan Motor Co. v. Nissan Computer Corp., 180 F. Supp. 2d 1089 (C.D. Cal. 2002).

[75] 39 Cal. 4th 95 (2006).

communication. Clear notice and implied consent are sufficient. "If, after being so advised, another party does not wish to participate in the conversation, he or she simply may decline to continue the communication."[76]

C. The Implications of *Kearney*

The Kearney case arose in the context of telephone monitoring, and there is a remarkable lack of case law addressing whether the California statute applies to Internet communications. If it does, or if there is one other state that applies its all-party consent rule to conduct affecting Internet communications across state lines, then no practical form of opt-in, no matter how robust, would save the practice of copying Internet content for behavioral advertising. That is, even if the ISP only copies the communications of those subscribers that consent, and the monitoring occurs only inside a one-party consent state, as soon as one of those customers has a communication with a non-consenting person (or Web site) in an all-party consent state that applies its rule to interceptions occurring outside the state, the ISP would seem to be in jeopardy. The ISP could not conceivably obtain consent from every person and Web site in the all-party consent state. Nor could it identify (for the purpose of obtaining consent) which people or Web sites its opted-in subscribers would want to communicate with in advance of those communications occurring.

A countervailing argument could be made that an all-party consent rule is not applicable to the behavioral advertising model, since the process only copies or divulges one half of the communication, namely the half from the consenting subscriber.

Conclusion

The practice that has been described to us, whereby an ISP may enter into an agreement with an advertising network to copy and analyze the traffic content of the ISP's customers, poses serious questions under the federal Wiretap Act. It seems that the disclosure of a subscriber's communications is prohibited without consent. In addition, especially where the copying is achieved by a device owned or controlled by the advertising network, the copying of the contents of subscriber communications seems to be, in the absence of consent, a prohibited interception. Affirmative express consent, and a cessation of copying upon withdrawal of consent, would probably save such practices under federal law, but there may be state laws requiring all-party consent that would be more difficult to satisfy.

[76] Id. at 118.